System for secure transactions

BACKGROUND OF THE INVENTION

The invention relates to a system for the execution of secure transactions in a multimedia network.

Multimedia networks like the Internet offer a wide variety of new possibilities, which will have a great impact on the business environment of the future. Various vendors will start to exploit the Internet as a marketplace. For a customer not to get lost within the vast amount of information that is provided, in the near future agent-based services shall be implemented. Agents are autonomous pieces of software, which may perform tasks for users on the Internet. Based on the user's preferences, they may assist the user in making a selection within the vast range of offered poducts. Complementary to this, the agent may assist in the actual purchase of such a product. As part of this process, the agent will have to be able to perform payments.

One of the biggest inhibitors on Electronic Commerce today is security. Consumers demand that their private information be kept private. When using agent technology within an E-Commerce service, adequate security precautions must be taken. At present, however, agent security is still in its infancy. Therefore, delegating payments to agents is not possible at this moment in time.

SUMMARY OF THE INVENTION

According to the present invention, an architecture is proposed in which agents may perform secure credit card payments. According to the invention, for the execution of such payments the SET (Secure Electronic Transactions) protocol is used, an upcoming standard for secure payments on the Internet by means of credit cards. All new entities and components that are necessary to provide agent-based SET payments will be defined and payment interaction (agent-agent, agent-user and other) will be elaborated upon.

Most entities of the standard infrastructure for performing SET-based payments by means of credit cards are straightforward analogies to real world credit card payments. A few, however, need further explanation. A brief description of these will be given first.

One of the main issues when providing secure payments is authentication of the involved entities. SET uses a robust set of digital certificates for this purpose. Each participant in a SET transaction requires a specific certificate or set of certificates that not only uniquely identifies this participant, but also attests to his or her privilege as holder of a payment card or as a holder of a Merchant account. Brand Associations (e.g. VISA/ MasterCard) or Card Issuers commission so called Certificate Authorities (CAs) to carry out the work of managing SET digital certificates.

Complementary to this, SET introduces the notion of a Payment Gateway, which is needed to validate SET digital certificates and preprocess authorisation, capture and settlement work concerning the payment at hand. Another fundamental requirement for performing SET payments is a component called an Electronic Wallet (E-Wallet). These wallets embody the SET protocol on the customer side and provide a means to store and manage the certificates to digitally sign messages, along with the security aspects consumers demand to keep private data private.

According to the present invention the task of performing SET credit card transactions is delegated to agents. In developing an infrastructure that enables this, the following constraints have been defined:

- Obtaining certificates is not a task that users will want to delegate to their agents. Furthermore, it is not very probable that banks and CAs will approve of this situation. Therefore, we assume all certificates and the E-Wallet to be in place.

- The standard SET infrastructure shall be kept intact.

Thereby the inherent security of SET payments shall remain present and the necessary alterations when implementing shall be limited.

Based on these constraints, an infrastructure has been designed wich will be discussed below.

EMBODIMENT OF THE INVENTION

Figure 1 shows an architecture in which the invention -the use the SET protocol by "secure agents- can be implemented. Figure 1 shows a multimedia network -the internet- 1. Connected to the internet 1 are customer PCs 2, and merchant servers 3, each via an internet service providers (ISP) 4. Also connected to the internet, via an ISP 4, is a payment (gateway) server 5. The payment server 5 is also - via an access server 6- connected to a "Banker's Interchange Network" (BIN) 7, having banking servers 8 connected to it.

A main issue in secure payments is authentication of entities. The SET protocol, to be used in the system shown in figure 1, uses a set of digital certificates for this purpose. Each participant in transaction requires a certificate that uniquely identifies the participant and also attests to his privilege as a holder of a account at the merchant server. Associations like VISA/MasterCard or other Card Issuers commission so called Certificate Authorities to carry out the work of managing SET digital certificates. In figure 1 a Trusted Third Party Server (TTPS) 9 of such Certificate Authority is connected to the internet 1 and can be approached by customers 2, merchants 3 and payment servers 5. Payment servers 5 are needed to validate the digital certificates and to preprocess authorisation, capture and settlement work concerning the payment.

Another fundamental requirement for performing SET payments is a system component called "Electronic Wallet" (EW) 10.

An E-wallet 10 embodies the SET protocol at the customer's side and provides means --within the customer's PC 2-- to store and manage the needed certificates, to digitally sign messages, along with the security aspects customers demand to keep private data private.

According to the invention agents are used to perform secure transactions. As said before, agents are autonomous pieces of software, which are enabled to perform tasks for users (customers or merchants). Based on preferences set by users 2 (customer) and 3 (merchant), the users' respective agents assists or represent the users in presenting and selecting of the merchants' products and, complementary to this, the users' respective agents assist or represents the users to purchase (collect) the selected products and to perform the secure payment for it.

Each customer 2 may be represented by a customer agent (CA), while each merchant 3 may be represented by a merchant agent (MA). The negotiation process (presentation, selection and collection of products and the payments for the collected products) is executed within an "agent platform", preferably embodied within an "Agent Negotiation Server" (ANS) 11. Communication between the customer's PC 3 and the customer's agent at the ANS's side is performed, at the customer's side via the E-wallet 10 --meant for SET based transaction-- which is extended with a special SET Agent Interface (SAI) 12.

The CA 13 communicates with the customer by means of the customer's "browser" (customer inferface) and, via the SAI 12, with the customer's E-Wallet 10 in order to initialise payments. As was the case according to the state-of-the-art (using credit cards), the actual SET payment process is performed between the E-Wallet 10 and the Merchant server 3. Therefore, during actual payment interaction the level of trust is the same as in known, credit card based SET payments.

The CA 13 will have to be authorised to initialise the EW 10 for payments. In standard SET transactions the customer is prompted --via the customer's browser-- to enter the E-Wallet password for this purpose. The CA 13 and the SAI 12 will have to be implemented such, that one of two scenarios may be performed: either the CA 13 has authorisation to release the cryptographic content of the E-Wallet 10 itself, or, after agent initialisation, the customer is prompted to provide an E-Wallet password. In the latter case, customer interaction is necessary. This is not desirable from a usability point of view, but might be preferred by customers (or merchants), since this will give them a sense of control over the payment.

Figure 2 shows a communication procedure for the system presented in figure 1.

For authentication and authorisation purposes, the CA 13 will carry a token, in which an authorisation code for opening up the E-Wallet is encapsulated. The level at which this token is secured within the agent depends on the location of the platform in which the CA 13 performs its tasks. If this platform resides on the customer PC, security requirements on both storing the token within the agent and communicating it to the E-Wallet are less strong than if the agent resides on a remote platform like the ANS 11 as suggested in figure 1. In the latter case, the token will need to be adequately secured, as will. communication between the agent and the E-Wallet. The security requirements are as follows:

The token is stored within the CA 13 in encrypted form, using a random key. A symmetric encryption scheme, such as DES, shall be applied here. This random key is generated at the PC 2 for each specific purchase. A new key shall be generated for each item that is to be bought by the agent.

For communication purposes, both the customer 2 and the CA 13 need to own a specific certificate, other than the

SET certificate. Payment start messages shall be communicated to the E-Wallet 10 in encrypted form, using a random session key. A symmetric encryption scheme, such as DES, shall be applied here. In turn, this random key shall be sent over in encrypted form, using the customer's public key related to the communication certificate. The message shall be signed with the agent's private key and a time stamp shall be added to the message in order to prevent replay by malicious parties.

In figure 2 the following communication steps are performed:

In step I, the CA 13 requests the Merchant Agent (MA) 14 to pay by credit card. The latter then informs the merchant server 3 of the requested payment, while parallell to that the CA 13 initialises the EW 10.

In step II, the standard SET procedure is performed by the EW 10, the Merchant server 3 and the Payment Gateway server 5.

Finally, in step III, after completion of the payment, the Merchant server 3 informs the MA 14 of this fact. The MA 14 passes this message on to the CA 13, which notifies the customer of payment completion.

The infrastructure and message flows are a natural extension of any agent-based infrastructure. Implementation may therefore by performed straightforwardly.